

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ESQUEMA NACIONAL DE SEGURIDAD (ENS) – CATEGORÍA MEDIA

los sistemas de información que dan soporte a las actividades de diseño, desarrollo, implantación, operación, mantenimiento y soporte de gestión empresarial en modalidad SaaS en la plataforma LEMATIC (incluyendo los módulos Lematic ERP/CRM, Lematic Hora y Lematic GO) según la declaración de aplicabilidad vigente.

DOCUMENTO PÚBLICO

IDENTIFICACIÓN Y CONTROL DOCUMENTAL

Organización	Lematic Innovation S.L	Código	POL-SEG-001
Versión	v1.0	Fecha de emisión	19/10/2026
Categoría del sistema	MEDIA	Autoridad de aprobación	Dirección
Entrada en vigor	Desde su aprobación		

Histórico de versiones

Fecha	Versión	Motivo	Aprobación
19/10/2026	v1.0	Emisión inicial del documento.	Dirección

Índice

1.	Introducción.....	4
2.	Objeto, finalidad y alcance.....	4
2.1.	Objeto y finalidad.....	4
2.2.	Alcance de aplicación.....	4
3.	Compromisos y principios de seguridad.....	5
3.1.	Compromiso de la Dirección.....	5
3.2.	Marco para los objetivos de seguridad.....	5
3.3.	Principios rectores.....	5
3.4.	Mínimo privilegio.....	6
3.5.	Mejora continua del proceso de seguridad.....	6
4.	Marco normativo y documental.....	6
4.1.	Marco normativo.....	6
4.2.	Marco documental.....	6
5.	Organización e implantación del proceso de seguridad.....	7
5.1.	Comité de Seguridad de la Información.....	7
5.2.	Roles y responsabilidades.....	8
5.3.	Designación y renovación de roles.....	8
5.4.	Resolución de conflictos.....	8
6.	Tratamiento de datos personales e información de clientes.....	8
7.	Análisis y gestión de riesgos.....	9
7.1.	Enfoque de gestión.....	9
7.2.	Medidas compensatorias.....	9
8.	Desarrollo documental de la política.....	9
9.	Gestión de personal.....	10
9.1.	Obligaciones del personal.....	10
10.	Terceras partes, prestadores y proveedores.....	10
11.	Profesionalidad.....	10
12.	Protección de las instalaciones.....	10
13.	Adquisición de productos de seguridad y contratación de servicios de seguridad.....	11
14.	Integridad y actualización del sistema.....	11
15.	Prevención ante otros sistemas de información interconectados.....	11
16.	Registro de la actividad y detección de código dañino.....	11
17.	Gestión de incidentes de seguridad.....	12
18.	Continuidad de la actividad.....	12
19.	Gestión documental, revisión y comunicación.....	12
19.1.	Autorización y control de accesos.....	12
19.2.	Control documental.....	12

19.3.	Protección de la información almacenada y en tránsito.....	13
19.4.	Comunicación y aplicación.....	13
19.5.	Revisión y mantenimiento	13
19.6.	Aprobación y entrada en vigor	13

1. Introducción

Lematic Innovation S.L integra la seguridad de la información en el gobierno y en la prestación de sus servicios los sistemas de información que dan soporte a las actividades de diseño, desarrollo, implantación, operación, mantenimiento y soporte de gestión empresarial en modalidad SaaS en la plataforma LEMATIC (incluyendo los módulos Lematic ERP/CRM, Lematic Hora y Lematic GO) según la declaración de aplicabilidad vigente. La protección alcanza la información relativa a la gestión empresarial de los clientes tratada por la plataforma Lematic (módulos ERP/CRM, Hora y GO), incluyendo datos identificativos, laborales, económico-financieros y contables, datos de carácter personal sujetos a RGPD y LOPDGDD, información fiscal conforme a la Ley 58/2003 General Tributaria, documentación mercantil conforme al Código de Comercio, datos derivados de las relaciones laborales conforme al Estatuto de los Trabajadores, así como metadatos, registros de actividad, credenciales de acceso y demás información técnica y operativa necesaria para la prestación del servicio SaaS.

La gestión de la seguridad se establece de forma proporcional a la MEDIA del sistema y se articula mediante responsabilidades definidas, gestión basada en riesgos, autorizaciones formales, documentación controlada, registros, gestión de incidentes, continuidad, control de terceros y revisión sistemática. El detalle operativo se desarrolla en la normativa, la arquitectura, los procedimientos y los registros específicos del sistema.

2. Objeto, finalidad y alcance

2.1. Objeto y finalidad

Lematic Innovation S.L establece un marco de gobierno y actuación de alto nivel para proteger la información y los servicios incluidos en el sistema ENS, preservando de forma proporcionada la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. El marco determina los compromisos de la Dirección, los principios de seguridad, las responsabilidades y las reglas generales que deben desarrollar los restantes documentos del sistema.

La finalidad es asegurar que las decisiones de seguridad sean coherentes con el alcance aprobado, la MEDIA, los riesgos identificados, las obligaciones aplicables y la capacidad real de la organización, evitando que la seguridad dependa de actuaciones aisladas o de decisiones no formalizadas.

2.2. Alcance de aplicación

El sistema ENS comprende la gestión empresarial mediante la plataforma Lematic en modalidad SaaS, integrando los módulos Lematic ERP/CRM, Lematic Hora y Lematic GO, junto con la infraestructura, aplicaciones, APIs y procesos de diseño, desarrollo, implantación, operación, mantenimiento y soporte asociados a dichos servicios. El alcance incluye el tratamiento, almacenamiento, transferencia y puesta a disposición de la información necesaria para prestar dichos servicios.

- datos de carácter personal de clientes y empleados, información económico-financiera y contable, documentación contractual y comercial, datos de gestión de recursos humanos y control horario, credenciales y datos de acceso de usuarios y administradores, código fuente y configuraciones técnicas de la plataforma, registros de actividad y logs del sistema, y demás información tratada por los módulos Lematic ERP/CRM, Lematic Hora y Lematic GO en el marco de la prestación del servicio SaaS.
- Dirección, responsables ENS, personal interno, administradores autorizados, terceros y resto de usuarios que intervienen en la prestación o soporte de los servicios incluidos.
- centro de trabajo de la organización, trabajo en movilidad mediante portátiles corporativos protegidos con conexiones externas cifradas (HTTPS/SSH) bajo supervisión y registro del Responsable técnico, y acceso remoto autorizado.
- OVHcloud, Debian 12, Plesk Obsidian, Apache y MySQL

Quedan fuera del alcance , así como custodia y transporte.

3. Compromisos y principios de seguridad

3.1. Compromiso de la Dirección

La Dirección asume la responsabilidad de impulsar y supervisar el sistema de seguridad, asegurar su coherencia con la actividad de Lematic Innovation S.L y establecer las condiciones necesarias para que la información y los servicios se protejan de acuerdo con la categoría MEDIA y los riesgos aplicables.

- Aprobar el marco de seguridad y mantenerlo alineado con el alcance y los servicios prestados.
- Designar formalmente los roles ENS y facilitar recursos humanos, técnicos, organizativos y económicos proporcionales a los riesgos.
- Velar por el cumplimiento de los requisitos legales, contractuales y de seguridad aplicables. Promover una gestión basada en riesgos, con tratamiento y seguimiento del riesgo residual conforme a los registros aplicables. Asegurar que los incidentes, la continuidad, las dependencias externas y las desviaciones de seguridad se gestionen dentro del sistema.
- Revisar los resultados relevantes y promover acciones de mejora cuando los riesgos, cambios o resultados del seguimiento lo requieran.

3.2. Marco para los objetivos de seguridad

Los objetivos de seguridad se establecerán dentro del ciclo de gestión ENS y deberán ser coherentes con la protección de la información, la continuidad de los servicios, la prevención y gestión de incidentes, el control de accesos, la gestión de terceros y la mejora continua. Cada objetivo deberá disponer de responsable, forma de seguimiento y evidencia adecuada en los registros del sistema.

Los objetivos se revisarán cuando cambien el alcance, los riesgos, los servicios, la tecnología, las relaciones con proveedores, las obligaciones aplicables o las necesidades de continuidad. Los valores cuantitativos de resultado se gestionan en los registros e indicadores correspondientes.

garantizar la confidencialidad, integridad y disponibilidad de la información tratada en la plataforma Lematic conforme a los requisitos del ENS para la categoría MEDIA, y promover la mejora continua del sistema de gestión de seguridad de la información mediante la revisión periódica de indicadores, auditorías y análisis de riesgos

3.3. Principios rectores

- Seguridad como proceso integral. La protección se considera durante la planificación, prestación, cambio y finalización de los servicios, y no como una actuación aislada.
- Gestión basada en riesgos. Las decisiones de seguridad se fundamentan en el Análisis y Registro de Riesgos ENS y en la criticidad de la información y de los servicios.
- Prevención, detección, respuesta y recuperación. Las medidas se orientan a reducir la probabilidad de incidentes, detectar anomalías, contener sus efectos y recuperar la operación.
- Proporcionalidad y defensa suficiente. Los controles y recursos se ajustan a la categoría MEDIA, al riesgo, al alcance y a las dependencias tecnológicas y contractuales.
- Necesidad de conocer, responsabilidad y trazabilidad. El acceso a información y recursos debe estar justificado por la función, quedar bajo responsabilidad identificada y generar la trazabilidad que corresponda.
- Seguridad durante el ciclo de vida. Las adquisiciones, cambios, operación, mantenimiento, retirada y relaciones con terceros deben considerar requisitos de seguridad desde su autorización hasta su cierre. Control de dependencias externas. Los servicios de terceros se gestionan atendiendo a responsabilidades, accesos, continuidad, seguridad contractual y evidencias disponibles.

3.4. Mínimo privilegio

Los permisos y privilegios se limitarán al nivel mínimo necesario para realizar las funciones autorizadas y prestar los servicios incluidos en el alcance. Las capacidades de administración, modificación, publicación, eliminación, exportación o acceso a información se concederán únicamente cuando resulten necesarias para la actividad asignada.

Las funciones administrativas se mantendrán diferenciadas de las tareas ordinarias en la medida que permita la tecnología y el modelo organizativo. Los privilegios se someterán a autorización, registro y revisión, y se retirarán o modificarán cuando cese la necesidad que justificó su asignación.

3.5. Mejora continua del proceso de seguridad

Lematic Innovation S.L mantendrá un proceso de mejora continua orientado a conservar la adecuación, eficacia y proporcionalidad del sistema. La mejora se apoyará en el análisis de riesgos, los indicadores, las auditorías, las revisiones técnicas, los incidentes, las vulnerabilidades, los cambios, las pruebas de continuidad y las evaluaciones de terceros.

Las desviaciones y oportunidades de mejora se analizarán y tratarán mediante actuaciones con responsabilidad y seguimiento definidos. Cuando corresponda, las conclusiones se trasladarán al análisis de riesgos, a la arquitectura, a la Declaración de Aplicabilidad, a los procedimientos, a las medidas compensatorias y a los registros afectados.

4. Marco normativo y documental

4.1. Marco normativo

La gestión de la seguridad de Lematic Innovation S.L se desarrolla teniendo como referencias normativas expresas, dentro de su ámbito de aplicación, las siguientes disposiciones:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
-

También se atenderán las obligaciones contractuales y los requisitos de seguridad asumidos frente a clientes, proveedores y terceros cuando resulten aplicables a los servicios incluidos en el alcance. Los cambios en estos requisitos se evaluarán y, cuando afecten al sistema, se trasladarán a la documentación, los riesgos, las autorizaciones y los controles correspondientes.

4.2. Marco documental

La seguridad se desarrolla mediante un conjunto coordinado de documentos y registros con distinto nivel de detalle. El nivel superior de gobierno es la Política de Seguridad de la Información y define los principios y responsabilidades; la Normativa Interna de Seguridad concreta las reglas obligatorias para personas usuarias, administradores y terceros; la Arquitectura de Seguridad describe los límites y dependencias del sistema; y los procedimientos regulan la ejecución controlada de las actividades de seguridad.

La trazabilidad operativa se conserva mediante registros específicos de activos, accesos, cambios y autorizaciones, incidentes, relaciones con terceros, indicadores, riesgos, medidas compensatorias, formación, comunicación y aceptación. Las evidencias técnicas se conservan en los soportes y registros previstos para cada actividad, sin sustituirse por la mera existencia de documentación normativa.

5. Organización e implantación del proceso de seguridad

La organización de la seguridad se apoya en la Dirección, en los roles ENS formalmente designados y en un Comité de Seguridad de la Información o mecanismo equivalente. La asignación de responsabilidades permite coordinar la protección de la información, las necesidades de servicio, la seguridad y la operación del sistema, manteniendo una estructura proporcional al tamaño y características de Lematic Innovation S.L.

5.1. Comité de Seguridad de la Información

El Comité de Seguridad de la Información o mecanismo equivalente estará integrado por los titulares de los roles ENS. Su función es coordinar las decisiones relevantes de seguridad, revisar riesgos y resultados de seguimiento, tratar incidentes, cambios significativos, continuidad y dependencias de terceros, y elevar a la Dirección aquellas decisiones que excedan sus competencias o respecto de las que no exista acuerdo. Además de las funciones indicadas el Comité de Seguridad deberá:

- Atender las inquietudes que, en materia de seguridad, se planteen desde la Dirección de la entidad y de los diferentes departamentos.
- Informar y ser informado regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información, con la aprobación de planes específicos.
- Elaborar la estrategia de evolución de la organización en lo que respecta a la seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Controlar periódicamente el grado de cumplimiento de las medidas propuestas para reducir el riesgo residual (pudiendo proponer acciones de mejora) y el correcto funcionamiento del procedimiento de gestión de incidentes, velando por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección (o por el órgano competente) y aprobar la Normativa de Seguridad de la Información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo/entidad en materia de seguridad.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque se respete el principio de seguridad desde el diseño, pudiendo requerir el asesoramiento del Responsable de la Seguridad, en todas aquellas iniciativas de la entidad que afecten a la seguridad de la información o de los sistemas. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas en el ámbito de aplicación del ENS.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

Las decisiones relevantes del mecanismo de coordinación conservan trazabilidad mediante actas, acuerdos, aprobaciones o evidencias equivalentes, de acuerdo con la naturaleza y relevancia de la cuestión tratada. Es el Responsable de la Seguridad quien actuará como Secretario del Comité de Seguridad, con las siguientes funciones derivadas:

- Convocar las reuniones del Comité de Seguridad de la Información, atendiendo a las instrucciones del presente Comité.
- Preparar los temas a tratar en las reuniones del Comité, recabando la información de los diferentes responsables.
- Elaborar el acta de las reuniones.

- Remitir el acta de las reuniones a los asistentes, recabando su firma.
- Conservar las actas, de acuerdo con los criterios de conservación documental de la entidad.

5.2. Roles y responsabilidades

Además de los roles y funciones descritos en la descripción de roles de seguridad, se destacan los siguientes roles así como parte de sus responsabilidades para las siguientes funciones:

Rol	Responsabilidad de alto nivel
Dirección	Aprobar la política, designar los roles ENS, proporcionar recursos proporcionales, supervisar el sistema y resolver los conflictos elevados.
Responsable de la Información	Determinar los requisitos de protección de la información, valorar las necesidades de seguridad y participar en las decisiones de riesgo.
Responsable del Servicio	Determinar los requisitos de seguridad y continuidad de los servicios incluidos en el alcance.
Responsable del Sistema	Gestionar la operación del sistema y aplicar las medidas, cambios y autorizaciones aprobadas.
Responsable de Seguridad	Coordinar la seguridad, el análisis de riesgos, el seguimiento de controles, los incidentes, la mejora y el asesoramiento a la Dirección.

5.3. Designación y renovación de roles

La Dirección designará formalmente a los titulares de los roles ENS mediante nombramiento, acuerdo o evidencia equivalente. La designación identificará el rol asignado y su ámbito de responsabilidad, y se conservará evidencia de la asignación y aceptación de los mismos.

La asignación se revisará y actualizará cuando exista sustitución, cambio organizativo, modificación del alcance, alteración relevante de las funciones o cualquier circunstancia que afecte a la capacidad de ejercer la responsabilidad asignada.

5.4. Resolución de conflictos

Los conflictos entre requisitos de protección de la información, necesidades del servicio, seguridad y operación del sistema se tratarán en el Comité de Seguridad de la Información o mecanismo equivalente. La decisión deberá considerar el riesgo, las obligaciones aplicables, la continuidad del servicio y las responsabilidades asignadas.

Cuando no exista acuerdo o la decisión exceda las competencias de los responsables implicados, la resolución corresponderá a la Dirección y quedará documentada mediante la evidencia de decisión que resulte apropiada.

6. Tratamiento de datos personales e información de clientes

La información de clientes y los datos personales tratados dentro del alcance se protegerán de acuerdo con su finalidad, necesidad de acceso, confidencialidad, integridad, conservación y uso autorizado. La protección de datos personales e información de clientes alcanza, entre otros elementos del alcance la plataforma Lematic trata datos personales e información de clientes propios de la gestión empresarial, laboral y comercial (datos identificativos, de contacto, económicos, contractuales y de recursos humanos de clientes, empleados y usuarios finales), gestionados a través de los módulos Lematic ERP/CRM, Lematic Hora y Lematic GO, sujetos a segregación por cliente, control de acceso basado en necesidad de conocer y protección conforme al RGPD y la LOPDGD.

El acceso se limitará a las personas que lo necesiten para la prestación del servicio. La transferencia, puesta a disposición y publicación de contenidos deberá realizarse mediante los canales y autorizaciones definidos, manteniendo la trazabilidad necesaria y evitando la divulgación, modificación, reutilización o publicación no autorizadas.

Los incidentes que afecten a datos personales o información de clientes se integrarán en el proceso general de gestión de incidentes, se coordinarán con las obligaciones contractuales y normativas que resulten aplicables y la correspondiente notificación a la Agencia Española de Protección de Datos (AEPD).

7. Análisis y gestión de riesgos

7.1. Enfoque de gestión

Las decisiones de seguridad se fundamentan en un análisis de riesgos del sistema y en un Registro de Riesgos que relaciona los escenarios identificados con los activos o servicios afectados, las amenazas, las salvaguardas, el tratamiento y el riesgo residual. El registro mantiene la trazabilidad de los riesgos identificados dentro del alcance y sirve de base para priorizar actuaciones, revisar controles y adoptar decisiones de aceptación cuando proceda.

El análisis se revisará dentro del ciclo de gestión ENS y ante cambios relevantes de alcance, tecnología, proveedores, servicios, incidentes, vulnerabilidades o requisitos aplicables. Las valoraciones, tratamientos y decisiones se conservan en el registro específico y no se sustituyen por declaraciones generales de cumplimiento.

7.2. Medidas compensatorias

Cuando una limitación objetiva impida aplicar una medida ordinaria en los términos previstos y exista una alternativa proporcional vinculada a un riesgo, la organización podrá mantener medidas compensatorias formalmente justificadas, con propietario, alcance, evidencia, criterio de eficacia y revisión definidos.

Las medidas compensatorias se gestionan en el Registro de Medidas Compensatorias y mantienen su relación con la Declaración de Aplicabilidad, los riesgos y los controles que justifican su existencia. Su continuidad depende de la revisión de eficacia y de la evolución del riesgo, sin que su mera documentación sustituya las evidencias técnicas u operativas requeridas.

8. Desarrollo documental de la política

El marco de seguridad se desarrolla y mantiene mediante documentación y registros específicos, de forma coordinada y sin duplicar innecesariamente el detalle operativo. Entre las piezas documentales relacionadas se incluyen:

la documentación se organiza de forma jerárquica y estructurada en un marco superior compuesto por la Política de Seguridad de la Información (POL-SGSI-001) y el Manual del SGSI (MSGSI-001), un nivel operativo integrado por procedimientos (PR-SGSI-XXX) e instrucciones técnicas (INS-SGSI-XXX), y un nivel de registros y evidencias formado por documentos de control operativo (REG-SGSI-XXX) y trazas de los sistemas fuente, manteniéndose toda la información documentada de forma controlada mediante título, código, versión, propietario y aprobador, y gestionándose a través de un repositorio digital controlado

Cada documento conservará su identificación, versión, responsabilidad y ámbito de aplicación. El nivel de detalle se mantendrá en el documento o registro al que corresponda, evitando trasladar configuraciones técnicas, resultados de auditoría o datos operativos a documentos de gobierno de alto nivel.

9. Gestión de personal

La seguridad asociada al personal se gestionará desde la incorporación hasta la modificación o finalización de sus funciones, atendiendo a las responsabilidades asignadas, al acceso a información y sistemas, a la necesidad de formación y a la revocación o modificación de autorizaciones cuando corresponda.

Las personas que intervengan en el alcance recibirán la información y formación necesarias para conocer sus obligaciones de seguridad y deberán mantener la diligencia, confidencialidad y responsabilidad exigibles en el uso de información, equipos, credenciales, servicios y plataformas.

9.1. Obligaciones del personal

- Cumplir la Política de Seguridad, la Normativa Interna y los procedimientos aplicables a su actividad.
- Utilizar únicamente los recursos, cuentas, servicios y accesos que hayan sido autorizados.
- Proteger las credenciales y la información, evitando su comunicación, almacenamiento, reutilización o exposición fuera de la finalidad autorizada.
- Respetar los criterios de mínimo privilegio, necesidad de conocer y separación de funciones aplicables.
- Comunicar sin demora los incidentes, pérdidas, accesos no reconocidos, anomalías o sospechas de compromiso que puedan afectar al sistema.
- Participar en las actividades de formación y concienciación establecidas y dejar constancia de la aceptación de las reglas que resulten aplicables.

10. Terceras partes, prestadores y proveedores

Los terceros que intervengan en el alcance deberán quedar sujetos a requisitos de seguridad proporcionales al servicio prestado, a la información tratada, a los accesos concedidos y a la dependencia que generen para la continuidad. Las responsabilidades, autorizaciones, condiciones de acceso, confidencialidad, trazabilidad y comunicación de incidentes se definirán en los contratos, acuerdos, procedimientos y registros que correspondan.

La organización mantendrá control sobre las relaciones externas que soportan el sistema, incluyendo OVHcloud, Debian 12, Plesk Obsidian, Apache y MySQL. La existencia de un servicio externo facilitada por un proveedor no traslada automáticamente a su fabricante o distribuidor, las responsabilidades de gobierno, autorización, configuración o uso que corresponden a Lematic Innovation S.L.

11. Profesionalidad

Las funciones que puedan afectar a la seguridad del sistema se encomendarán a personas o proveedores autorizados con conocimientos y capacidad acordes con la responsabilidad asignada. La organización procurará que los responsables ENS, administradores y personal que maneje información o recursos del alcance mantengan la competencia necesaria para aplicar las reglas y procedimientos que les correspondan.

La formación inicial, la concienciación y la actualización de conocimientos se integrarán en la gestión del personal. Las actuaciones administrativas o técnicas con impacto relevante deberán quedar reservadas a perfiles autorizados y realizarse dentro del marco de responsabilidades, autorizaciones y evidencias definido por el sistema.

12. Protección de las instalaciones

Las instalaciones y ubicaciones en las que se encuentren equipos, soportes o información del sistema están protegidas frente al acceso o manipulación no autorizados y frente a circunstancias que puedan afectar a la disponibilidad o integridad de los recursos. El nivel de protección física se establecerá de forma proporcional al riesgo, al tipo de activo y al contexto de uso.

El acceso a los elementos que soportan funciones críticas se limitará a personal autorizado. Las intervenciones, traslados, mantenimientos y actuaciones que puedan afectar a equipos o soportes deberán sujetarse a autorización y trazabilidad cuando su relevancia lo requiera. Las limitaciones físicas identificadas se gestionarán mediante los riesgos y medidas aprobados en los registros correspondientes.

13. Adquisición de productos de seguridad y contratación de servicios de seguridad

La incorporación de productos, componentes, software o servicios que puedan afectar al sistema estarán sometidas a una evaluación previa y proporcional de seguridad. La decisión considerará la finalidad, la capacidad de configuración segura, el soporte y actualización, la trazabilidad disponible, la compatibilidad con los mecanismos de protección requeridos y las garantías del proveedor que resulten relevantes para el uso previsto.

Cuando resulte aplicable un requisito de utilización de componentes cualificados o incluidos en catálogos de referencia CPSTIC, se verificará dicha condición antes de la adquisición. Cuando proceda, la organización realizará la correspondiente taxonomía y aplicará la medida compensatoria correspondiente, dejando la trazabilidad correspondiente en los procedimientos y registros de proveedores, cambios, activos y medidas compensatorias.

14. Integridad y actualización del sistema

La configuración, modificación y actualización de los componentes del sistema se realizará bajo responsabilidad de personal autorizado y conforme a los procedimientos de configuración y gestión de cambios. Se procurará mantener los elementos en condiciones compatibles con los requisitos de seguridad, evitando el uso de configuraciones, software o componentes cuya procedencia, soporte o estado no permitan una gestión razonable del riesgo.

Los cambios relevantes deberán ser autorizados, registrados y comprobados en función de su impacto. La gestión de vulnerabilidades, actualizaciones, parches, software autorizado y retirada de componentes obsoletos se coordinará con el inventario, los riesgos, las incidencias y las evidencias técnicas aplicables.

15. Prevención ante otros sistemas de información interconectados

Las interconexiones con otros sistemas de información estarán sujetas a un proceso formal de autorización, evaluación y control que garantice que su establecimiento y operación no introduzcan riesgos no aceptables para la seguridad de la información.

Dicho proceso contemplará, al menos, la identificación de los sistemas interconectados, la delimitación de responsabilidades, el análisis de riesgos, la definición de los mecanismos de protección necesarios, el control de los accesos y flujos de información, la trazabilidad de las comunicaciones y la revisión periódica de las condiciones de seguridad aplicables.

La puesta en servicio, modificación o mantenimiento de cualquier interconexión deberá realizarse conforme al procedimiento establecido por la organización y quedar adecuadamente documentada.

16. Registro de la actividad y detección de código dañino

La organización mantendrá la trazabilidad necesaria sobre accesos, actuaciones administrativas y eventos de seguridad relevantes en los sistemas y servicios incluidos en el alcance, de acuerdo con las capacidades disponibles y con los procedimientos de accesos, monitorización e incidentes. Los registros deberán protegerse frente a alteraciones o accesos no autorizados y utilizarse para apoyar la detección, análisis y reconstrucción de hechos cuando resulte necesario.

Los equipos y servicios se gestionarán con mecanismos de prevención y detección de código dañino adecuados a su función y exposición. La aparición de alertas, comportamientos anómalos o indicios de compromiso deberá integrarse en el proceso de gestión de incidentes y generar las actuaciones de contención, recuperación y revisión que correspondan.

17. Gestión de incidentes de seguridad

Los incidentes de seguridad se identificarán, comunicarán, registrarán, analizarán, contendrán, resolverán y revisarán de forma coordinada. El personal y los terceros autorizados deberán comunicar las anomalías o hechos que puedan comprometer la información o los servicios, y el Responsable de Seguridad coordinará su tratamiento dentro del ámbito de sus responsabilidades.

La gestión de cada incidente mantendrá relación con los activos, servicios, cambios, proveedores, continuidad y riesgos afectados. La trazabilidad se conservará en el registro de incidentes de seguridad y en las evidencias asociadas. Las conclusiones relevantes se utilizarán para corregir causas, mejorar controles y actualizar la gestión de riesgos cuando proceda.

18. Continuidad de la actividad

La continuidad se gestionará atendiendo a la criticidad de los servicios, la información, las dependencias tecnológicas y humanas, la capacidad disponible y las relaciones con proveedores. El análisis de impacto y los criterios de recuperación se mantendrán coordinados con las copias, restauraciones, capacidad, incidentes y riesgos del sistema.

Las estrategias y actuaciones de recuperación deberán ser proporcionales al escenario de interrupción y mantenerse sujetas a pruebas y revisión. Los resultados de las pruebas, restauraciones, incidencias y actuaciones de recuperación se conservarán en los registros específicos y se utilizarán para revisar las dependencias, prioridades y medidas de continuidad.

19. Gestión documental, revisión y comunicación

La documentación de seguridad se mantendrá identificada, controlada, accesible para las personas que la necesiten y protegida frente a modificaciones no autorizadas. La gestión documental deberá permitir conocer la versión vigente, su autoridad de aprobación, el ámbito de aplicación y los registros o documentos que desarrollan cada materia.

19.1. Autorización y control de accesos

El acceso a información, servicios, equipos y funciones administrativas requerirá autorización conforme a la necesidad del servicio y al principio de mínimo privilegio. Las altas, modificaciones, privilegios, revisiones y bajas se mantendrán trazables mediante los registros y procedimientos aplicables.

La existencia de una cuenta, dispositivo, funcionalidad o relación contractual no implicará autorización automática para utilizarla. Los accesos deberán revisarse ante cambios de función, finalización de la necesidad, incidentes o cualquier circunstancia que pueda alterar su justificación.

19.2. Control documental

Los documentos del sistema mantendrán identificación, código o denominación, versión, fecha de emisión y autoridad de aprobación. La organización conservará la trazabilidad de sus revisiones, evitará el uso no controlado de versiones obsoletas y limitará la modificación de documentación a personas autorizadas.

Los registros de ejecución y las evidencias técnicas se conservarán en los soportes definidos para cada proceso. La documentación de gobierno no se utilizará como sustituto de las evidencias de funcionamiento, configuración, revisión o ejecución que deban existir para demostrar la aplicación de las medidas.

19.3. Protección de la información almacenada y en tránsito

La información del alcance se almacenará, transferirá y pondrá a disposición mediante ubicaciones, servicios y canales autorizados, aplicando criterios de necesidad de conocer, confidencialidad, integridad y trazabilidad acordes con su uso. Las transferencias deberán limitarse a la información necesaria y realizarse con destinatario y finalidad identificados.

Código propio de la herramienta LEMATIC; Información documental, evidencia y trazas electrónicas; Información de productos, almacenes y trazabilidad logística; Información de proyectos, producción y prestación de trabajos; Información laboral, horaria y de presencia; Información económica, contable, fiscal y de facturación; Información comercial; y CRM; Información de clientes, proveedores y contactos. se mantendrán bajo los controles de acceso y custodia definidos. La selección de mecanismos técnicos de protección se desarrolla en la arquitectura, los procedimientos y las configuraciones autorizadas, sin establecer en el nivel de gobierno especificaciones técnicas no consolidadas.

19.4. Comunicación y aplicación

El marco de seguridad de alto nivel y la Normativa Interna de Seguridad se comunicarán o pondrán a disposición del personal, administradores y terceros a quienes resulten aplicables. La organización mantendrá evidencia de la comunicación, formación y aceptación que corresponda, de modo que las personas afectadas conozcan sus responsabilidades antes de utilizar los recursos o acceder a la información del sistema.

Las condiciones contractuales y de acceso de terceros deberán ser coherentes con este marco y con los procedimientos específicos que regulen proveedores, credenciales, accesos, transferencias, continuidad e incidentes.

19.5. Revisión y mantenimiento

La Dirección revisará periódicamente el marco de seguridad y, adicionalmente, cuando existan cambios relevantes en el alcance, los servicios, la información, la tecnología, los proveedores, los riesgos, los incidentes, las auditorías o los requisitos aplicables. La revisión deberá comprobar que las responsabilidades, principios y referencias documentales siguen siendo adecuados y coherentes con la realidad de la organización.

Los cambios aprobados se incorporarán bajo control de versión y se comunicarán a las personas afectadas cuando modifiquen obligaciones, responsabilidades o condiciones de uso.

19.6. Aprobación y entrada en vigor

La aprobación corresponde a la Dirección de Lematic Innovation S.L. La versión aprobada entrará en vigor desde la formalización de dicha aprobación y mantendrá su vigencia hasta que sea sustituida por una revisión posterior o se acuerde expresamente su retirada.

La organización conservará la evidencia formal de aprobación, la versión vigente y la trazabilidad de su publicación o puesta a disposición. Cualquier modificación deberá seguir el mismo criterio de control, aprobación y comunicación.

APROBACIÓN

Autoridad de aprobación	Dirección
Entrada en vigor	19/10/2026
Firma	Firmado por ***3351** JOSEFA FRESNEDA (R: ****7708*) el día 26/10/2026 con un certificado emitido por AC Representación